كيف تتجنب الاستهداف؟

اعداد

د. أحمد المغربي

محامي ومستشار قانوني.



سلسلة الامتثال في إدارة القضايا المصيرية المعاصرة
سلسلة فكرية – تحليلية تُعالج الامتثال والحوكمة في:
الحركات، المؤسسات، القرار العام، والصراع السياسي.

كيف تتجنب الاستهداف؟

القسم الأول: المادة النظرية.

القسم الثاني: مثال تطبيقي من لبنان (تفجير البيجرات والوكي توكي).

إعداد

د. أحمد المغربي

دكتوراه قانون – مستشار قانوني – محامي –

دورة (CAMS) مكافحة جرائم غسيل الأموال وتمويل الإرهاب

إسطنبول، الأربعاء 2026/03/25م

المحتويات

	ثالثا/ كاميرات الطائرات المسيّرة فوق الضاحية. رابعا/ اختراق جهاز ذكي داخل الغرفة. **السؤال السادس: ما هي خطة الحماية العملية لمنع تكرار هذه الاغتيالات؟** الدائرة الأولى: حماية المعلومات قبل الوصول. الدائرة الثانية: حماية المبنى. الدائرة الثالثة: الحماية أثناء الاجتماع. الخلاصة.		

كيف تتجنب الاستهداف؟

تمهيد:

تتوالى حوادث استهداف الأشخاص (الطبيعيين و/ أو المعنويين) – بطريقة مميتة – من قبل الكيان الصهيوني بالذات وبشكل مباشر، و/ أو من قبل داعميه بشكل غير مباشر (وهم كثير)، وغالبا نتيجة الاستهداف شهداء، وجرحى، وتدمير وتهجير.

وحيث ان الوقاية من الاستهداف تصبح ضرورة ملحة لعدد كبير من الأشخاص الذين يمكن ان يتعرضوا للاستهداف، وقد يكونوا غير تابعين الى أي تنظيم او فصيل او حركة، بل استهداف لشبهة تعامل أو تزويد أغذية أو غيرها مما لا يعد جريمة بحد ذاتها، وإنما فقط لأنها موجهة إلى المحاصرين من المدنيين.

ولأن الحماية من الاستهداف هو علم بحد ذاته مبني على معرفة الكثير من الأدوات والإجراءات التي يقوم عليها الاستهداف، ولأن معرفة تجنب الاستهداف يصبح بمنزلة الفرض على بعض الأشخاص (إن لم يكن كذلك على القاطنين في مناطق النزاع والتعرض الخطر)؛ بذلك يصبح على بعض الأشخاص (والأفضل الجميع) البحث والكشف عن كيفية تجنب الاستهداف، وجعلها ثقافة له ولأفراد عائلته وللمقربين والمتعاملين معه.

هذا الموضوع لا يشمل جميع الإجراءات والأدوات، بل ينمي روح الاكتشاف ومتابعة أحدث التطورات والتقنيات في ذات المجال، إذ لا يكف البشر عن إيجاد الأدوات والتقنيات والإجراءات للوصول إلى الشخص او المجموعة المراد الإيقاع بها قتلا و/ أو أسرا و/ أو ايذاء.

ولأن الاستهداف غالبا لا يفرق بين الشخص ومن حوله من الأبرياء، سواء معارف وأقارب أم غير ذلك، فإن ذلك يجعل من ثقافة تجنب الاستهداف ضرورة للجميع في مناطق النزاع القائم أو المحتمل، ما يقلل من الأضرار سواء على مستوى الجماعات المنظمة أم على الأبرياء المواطنين والموجودين.

وفي هذه الورقة، فإننا لا نحدد جهة ما لتوجيه الخطاب اليها، ولكن يشمل كل مجموعة منظمة سواء كانت جماعة أم جمعية أم تنظيم أم حركة أم شخص معنوي عام أم شخص معنوي خاص أم شخص طبيعي، لذلك فهذه الورقة موضوعة للجميع، مع أن حركات المقاومة في منطقة الشرق الأوسط هي الأكثر استهدافا من بقية مناطق العالم، وكذلك المواطنين العاديين الذين يسمونهم بالأضرار الجانبية حال اصابتهم، وإن كان الواضح أنهم مستهدفون لذواتهم لدخولهم ضمن إطار سياسة التهجير التي يتم تداولها علنا، ولأنهم يريدون مناطق خالية تماما من السكان.

ويجدر الإشارة هنا إلى قناة موجودة على تطبيق التيليجرام تبين الكثير من طرائق وأدوات الحرص على السلامة الشخصية والجمعية، ولديها الكثير من التجارب التي تؤيد بها إجراءات الأمن والسلامة من الاستهداف، وهذه القناة أسمها: (الحارس)، يجدر بكل شخص أن يجعل له زيارتها ورد يومي له ولو بمقدار (10) دقائق كفيلة بتزويده بإجراءات الحماية من الاستهداف له شخصيا ولمن حوله ولأبناء الوطن.

تم تقسيم هذه الورقة إلى قسمين:

القسم الأول: القسم النظري.

القسم الثاني: القسم التطبيقي (ما حدث في الضاحية الجنوبية من تفجيرات البيجرات والوكي توكي في سبتمبر 2024).

نتناول الموضوع بأسلوب السؤال والجواب، وفق الآتي:

القسم الأول: القسم النظري

نتناول الموضوع من خلال الإجابة عن السؤالين الآتيين:

السؤال الأول: شاهدنا الأيام الماضية كيف يتم استهداف شخصيات كثيرة بصواريخ وبغيرها، فكيف يتم تحديد الشخص المستهدف؟ وكيف يعرف انه مستهدف؟ وكيف يحمي نفسه من الاستهداف؟

السؤال الثاني: إذا شعر الشخص انه مستهدف، ما هي الاجراءات التي يتخذها لحماية نفسه أولا، ثم عائلته الملازمين له؟

وتاليا الشرح:

السؤال الأول: شاهدنا الأيام الماضية كيف يتم استهداف شخصيات كثيرة بصواريخ وبغيرها، فكيف يتم تحديد الشخص المستهدف؟ وكيف يعرف انه مستهدف؟ وكيف يحمي نفسه من الاستهداف؟

الجواب:

أولا/ كيف يتم تحديد الشخص المستهدف؟

1-المراحل الاستخباراتية لتحديد الهدف:

أ) مرحلة جمع معلومات عن الشخص المستهدف:

- **المراقبة:** مراقبة الحركات اليومية، الأماكن التي يزورها.
- **التجسس:** التنصت على المكالمات، مراقبة الاتصالات.
- **الاستخبارات:** جمع معلومات من المصادر المختلفة (عملاء، تقنية).
- **التحليل:** تحليل البيانات وتحديد الأهمية الاستراتيجية.

ب) مرحلة التقييم:

- **الأهمية العسكرية:** تقييم دور الشخص في المقاومة.
- **الأهمية السياسية:** تقييم تأثير الشخص في الرأي العام.
- **الأهمية الأمنية:** تقييم دور الشخص في الأمن.
- **الأهمية النفسية:** تقييم تأثير استهدافه على الجمهور.

ج) مرحلة الموافقة:

- **موافقة القيادة العليا:** موافقة القيادة السياسية والعسكرية على تنفيذ الاستهداف.
- **تقييم المخاطر:** تقييم المخاطر من الاستهداف.
- **توقيت العملية:** اختيار التوقيت المناسب.
- **وسيلة الاستهداف:** اختيار الوسيلة المناسبة (صاروخ، طائرة، غيرها).

2-مصادر المعلومات لتحديد الهدف المستهدف:

أ) المصادر التقنية:

- **التجسس الإلكتروني:** تنصت على الاتصالات، مراقبة النشاط الرقمي.
- **الأقمار الصناعية:** مراقبة الحركات، تتبع المواقع، ....
- **الطائرات دون طيار:** مراقبة الأماكن، تصوير العمليات، .....
- **أنظمة المراقبة:** أنظمة المراقبة الذكية، أنظمة التعرف على الوجوه، .....

ب) المصادر البشرية:

- **العملاء:** عملاء داخل الجماعة أو الحركة، عملاء في الأماكن التي يزورها، .....
- **المخبرون:** مخبرون في الأماكن التي يعمل فيها.
- **الخبراء:** خبراء في تحليل الشخصيات، خبراء في الاستهداف، ....

ج) مصادر أخرى:

- **الوسائط الاجتماعية:** تحليل النشاط على وسائل التواصل.
- **الأنشطة العامة:** تحليل الأنشطة التي يحضرها ومراقبتها.
- **العلاقات الشخصية:** تحليل العلاقات الشخصية والسياسية التي يتعامل معها ومراقبتها.

ثانيا/ كيف يعرف الشخص أنه مستهدف؟

أ) علامات التهديد المباشر:

- **تحذيرات مباشرة:** رسائل تحذير بريدية او واتس اب او ما سنجر او غيرها، تحذيرات عبر القنوات.
- **محاولات اغتيال:** محاولات اغتيال فاشلة سابقة.
- **الاستهداف العائلي:** استهداف الأفراد المقربين منه.
- **المراقبة المباشرة:** شعور بالمراقبة، ملاحظة أشخاص غامضين، ....

ب) علامات التهديد غير المباشر:

- **التحركات غير الطبيعية:** زيادة في التحركات الأمنية المحيطة.
- **التغييرات في الروتين:** تغيير في الروتين اليومي من الأشخاص الذين يمكن ان يكونوا مجندين للملاحقة.
- **التنبيهات الأمنية:** تنبيهات من جهات أمنية.
- **المعلومات الاستخباراتية:** معلومات من مصادر موثوقة (معلومة أو تحليل استخباراتي مهني).

ج) علامات التحذير الذاتي:

- **الشعور بالخطر:** شعور داخلي بالخطر (يتشكل هذا الشعور بنتيجة ما تم ذكره أعلاه من تنبيهات وإجراءات).
- **التحقق من المعلومات:** التحقق من المعلومات من مصادر متعددة.
- **الاستعداد للأزمات:** الاستعداد للأزمات، وجود خطط طوارئ.
- **التحقق من الأمان:** التحقق من إجراءات الأمن الشخصية بشكل مستمر (يزيد خلال الأزمات).

ثالثا/ كيف يحمي الشخص نفسه من الاستهداف؟

أ) الإجراءات الوقائية:

1) تغيير الروتين اليومي:

- **تغيير المواقع:** تغيير أماكن الإقامة بشكل آمن، تغيير الأماكن التي يزورها.
- **تغيير الأوقات:** تغيير الأوقات التي يذهب فيها إلى الأماكن المعتادة.
- **تغيير الطرق:** تغيير الطرق التي يسلكها.
- **تغيير الاتصالات:** تغيير أنواع الاتصالات.

2) تعزيز الأمن الشخصي:

- **مرافقة أمنية:** وجود مرافقة أمنية دائمة.
- **التخفي:** استخدام وسائل التخفي (نقاب، نظارات، ملابس).
- **التنقل السريع:** التنقل بسرعة، تغيير المواقع بسرعة.
- **الاستخدام التقني:** استخدام أجهزة تخفي تقنية.

3) تعزيز الأمن الرقمي:

- **تشفير الاتصالات:** تشفير الاتصالات، استخدام تطبيقات آمنة.
- **تغيير الأرقام:** تغيير الأرقام، عدم استخدام أرقام معروفة.
- **تجنب التواصل العلني:** تجنب التواصل العلني، عدم الإفشاء بمواقع.
- **الاستخدام الآمن:** استخدام الإنترنت بشكل آمن.

ب) الإجراءات الاستباقية:

1) وجود خطط طوارئ:

- **خطوط هروب:** وجود خطوط هروب محددة مسبقاً.
- **ملاذات آمنة:** وجود ملاذات آمنة معروفة مسبقاً.
- **اتصالات طوارئ:** وجود اتصالات طوارئ معروفة.
- **خطة عمل:** خطة عمل في حالة الاستهداف.

2) تدريب خاص:

- **تدريب عسكري:** تدريب عسكري على أساسيات الحماية.
- **تدريب على التخفي:** تدريب على أساسيات التخفي والتنقل.
- **تدريب على الرد:** تدريب على الرد على الهجمات.
- **تدريب على النجاة:** تدريب على أساسيات النجاة.

3) الاستعداد النفسي:

- **الصبر:** الصبر والتحمل في الظروف الصعبة.
- **التوكل:** التوكل على الله، الثقة بالنفس.
- **التحدي:** التحدي في وجه الهجمات.
- **الاستعداد النفسي:** الاستعداد النفسي للمواجهة.

ج) الإجراءات أثناء الاستهداف:

1) التخفي الفوري:

- **الاختباء:** الاختباء فوراً عند سماع التحذيرات.
- **التنقل:** التنقل فوراً إلى مكان آمن.
- **الإبلاغ:** الإبلاغ فوراً للجهات المختصة بطريقة آمنة من التتبع.
- **الاستعداد:** الاستعداد للمواجهة.

2) المواجهة:

- **الدفاع عن النفس:** الدفاع عن النفس بكل الوسائل المتاحة.
- **المساعدة:** طلب المساعدة من الجهات المختصة.

- **الانسحاب:** الانسحاب إلى مكان آمن.
- **الرد:** الرد على الهجوم بفعالية.

3) بعد الاستهداف:

- **الإبلاغ:** الإبلاغ للجهات المختصة.
- **التقييم:** تقييم الوضع، تحليل الهجوم.
- **التعلم:** تعلُم الدروس، تحسين الإجراءات.
- **الاستمرارية:** الاستمرارية في العمل، عدم التوقف.

4) نصائح عملية:

أ) نصائح يومية:

- **التغيير المستمر:** تغيير الروتين يومياً.
- **المراقبة:** مراقبة المحيط دائماً.
- **التحقق:** التحقق من المعلومات قبل تصديقها واعتمادها.
- **الاستعداد:** الاستعداد دائماً للأزمات.

ب) نصائح أمنية:

- **السرية:** الحفاظ على السرية في كل الأوقات.
- **الحيطة:** الحيطة والحذر في كل الأماكن.
- **التحذير:** الاستماع إلى التحذيرات دائماً.
- **الاستعداد:** الاستعداد للمواجهة دائماً.

ج) نصائح نفسية:

- **الهدوء:** الحفاظ على الهدوء في المواقف الصعبة.
- **الثقة:** الثقة بالنفس والقدرة على المواجهة.
- **التوكل:** التوكل على الله في كل الأوقات.
- **الصبر:** الصبر في وجه الصعوبات.

رابعا/ الخلاصة:

أ) تحديد الهدف من قبل الجهة المقصودة عملية معقدة تستخدم فيها أحدث الأساليب الاستخباراتية.

ب) معرفة الشخص أنه مستهدف يعتمد على قدرته الشخصية و/ أو الأشخاص المحيطين به او العاملين معه على ملاحظة العلامات والتحذيرات.

ج) حماية النفس تعتمد على الإجراءات الوقائية والاستباقية والقدرة على المواجهة.

د) الاستعداد هو مفتاح نجاح الحماية في كل الأوقات.

السؤال الثاني: إذا شعر الشخص انه مستهدف، ما هي الاجراءات التي يتخذها لحماية نفسه أولا، ثم عائلته الملازمين له؟

الجواب:

أولا/ الإجراءات الفورية لحماية الشخص نفسه:

1- الإجراءات الأولية (دقائق إلى ساعات):

أ) تغيير الموقع فوراً:

- **التنقل السريع:** الخروج من الموقع الحالي فوراً (لا أكثر من 5 دقائق).
- **التنقل إلى مكان معد معروف سابقاً:** مكان معروف للشخص فقط وليس للآخرين.
- **التنقل إلى مكان مزدحم:** مكان به كثير من الناس (أسواق، مستشفيات، جامعات).
- **التنقل إلى مكان آمن:** مكان معروف له أمنياً (مقار الحركة، منازل أصدقاء موثوقين).

ب) قطع الاتصالات:

- **إطفاء الهاتف:** إطفاء الهاتف تماماً (وليس وضع الطيران فقط).
- **إزالة البطاقة:** إزالة بطاقة SIM فوراً.
- **عدم استخدام الإنترنت:** عدم استخدام أي اتصال بالإنترنت.
- **البقاء في وضع الصمت:** عدم إصدار أي صوت أو حركة.

ج) تغيير مظهر الشخص:

- **التخفي الفوري:** تغيير الملابس فوراً (الملابس الداخلية، القبعات، النظارات).
- **استخدام الأدوات:** استخدام أدوات التخفي (نقاب، نظارات، قبعات).
- **تغيير الملامح:** استخدام مستحضرات التجميل لتغيير الملامح.
- **التنقل بشكل مختلف:** التنقل بشكل مختلف (مشي بدلاً من السيارة، سيارة بدلاً من المشي).

2-الإجراءات في الساعات الأولى:

أ) البحث عن ملجأ آمن:

- **العودة إلى مقر الحركة:** العودة إلى مقر الحركة الرئيسي.
- **الذهاب إلى منزل آمن:** الذهاب إلى منزل معروف آمناً.
- **الإقامة في مكان مزدحم:** الإقامة في مكان به كثير من الناس.
- **الإقامة في مكان معروف:** مكان معروف له أمنياً.

ب) الاتصال بالجهات الأمنية:

- **الإبلاغ الفوري:** الإبلاغ للجهات الأمنية فوراً.
- **تقديم المعلومات:** تقديم المعلومات المتوفرة (الموقع، الوقت، التفاصيل).
- **طلب المساعدة:** طلب المساعدة من الجهات الأمنية.
- **التنسيق:** التنسيق مع الجهات الأمنية.

ج) الاستعداد للمواجهة:

- **التحرك بشكل سريع:** التحرك بشكل سريع إلى مكان آمن.
- **الاستعداد للدفاع:** الاستعداد للدفاع عن النفس.
- **الاستعداد للهروب:** الاستعداد للهروب فوراً.
- **الاستعداد للمواجهة:** الاستعداد للمواجهة بكل الوسائل المتاحة.

ثانيا/ الإجراءات لحماية العائلة الملازمة:

1- الإجراءات الفورية لحماية العائلة:

أ) إخلاء العائلة فوراً:

- **إخلاء الموقع فوراً:** إخلاء الموقع الحالي فوراً (لا أكثر من 5 دقائق).
- **إرسال العائلة إلى مكان آمن:** إرسال العائلة إلى مكان معروف آمناً معد مسبقا.
- **إرسال العائلة إلى مقر الحركة:** إرسال العائلة إلى مقر الحركة الرئيسي.
- **إرسال العائلة إلى منزل معروف:** إرسال العائلة إلى منزل معروف آمناً.

ب) حماية العائلة أثناء التنقل:

- **مرافقة عسكرية:** مرافقة عسكرية للعائلة أثناء التنقل.
- **التنقل السريع:** التنقل السريع إلى مكان آمن.
- **التنقل بشكل مخفي:** التنقل بشكل مخفي (سيارات عادية، ملابس عادية).
- **التنقل في أوقات مختلفة:** التنقل في أوقات مختلفة عن المعتاد.

ج) إخفاء هوية العائلة:

- **تغيير مظهر العائلة:** تغيير مظهر العائلة فوراً (ملابس، قبعات، نظارات).
- **إخفاء الهويات:** إخفاء هويات العائلة (بطاقات هوية، أوراق).
- **استخدام أسماء مستعارة:** استخدام أسماء مستعارة للعائلة.
- **عدم الإفشاء بمعلومات:** عدم الإفشاء بمعلومات عن العائلة.

2- إجراءات تأمين مكان إقامة العائلة:

أ) اختيار مكان آمن:

- **اختيار مكان معروف:** مكان معروف آمناً للعائلة.
- **اختيار مكان بعيد:** مكان بعيد عن المعتاد عن عمل الشخص.
- **اختيار مكان مزدحم:** مكان به كثير من الناس.

ب) تأمين المكان:

- **تأمين المداخل:** تأمين جميع المداخل والمخارج.
- **تأمين النوافذ:** تأمين جميع النوافذ والفتحات.
- **تأمين الأسطح:** تأمين جميع الأسطح والطوابق.
- **تأمين الأبواب:** تأمين جميع الأبواب والمداخل.

ج) تأمين الاتصالات:

- **تشفير الاتصالات:** تشفير جميع الاتصالات للعائلة.
- **تغيير الأرقام:** تغيير جميع أرقام الاتصالات للعائلة.
- **عدم استخدام الإنترنت:** عدم استخدام أي اتصال بالإنترنت للعائلة.
- **استخدام قنوات آمنة:** استخدام قنوات اتصالات آمنة للعائلة.

3- الإجراءات طويلة الأمد لحماية العائلة:

أ) إعادة تأمين المكان:

- **الإقامة في مكان جديد:** الإقامة في مكان جديد معروف آمناً.
- **تغيير المكان بشكل دوري:** تغيير المكان بشكل دوري (كل أسبوع أو شهر).

- **الإقامة في مكان معروف:** الإقامة في مكان معروف أمنياً للعائلة.
- **الإقامة في مكان بعيد:** الإقامة في مكان بعيد عن المعتاد عن عمل الشخص.

ب) إعادة تأمين الاتصالات:

- **تغيير الاتصالات:** تغيير جميع الاتصالات للعائلة.
- **استخدام قنوات آمنة:** استخدام قنوات اتصالات آمنة للعائلة.
- **عدم الإفشاء بمعلومات:** عدم الإفشاء بمعلومات عن العائلة.
- **الاستخدام الآمن:** استخدام الإنترنت بشكل آمن للعائلة.

ج) إعادة تأمين المظهر:

- **تغيير المظهر:** تغيير مظهر العائلة بشكل دوري.
- **استخدام ملابس عادية:** استخدام ملابس عادية للعائلة.
- **استخدام أدوات التخفي:** استخدام أدوات التخفي للعائلة.
- **عدم الإفشاء بمعلومات:** عدم الإفشاء بمعلومات عن العائلة.

ثالثا/ الإجراءات المشتركة لحماية الشخص وعائلته:

1- الإجراءات التنظيمية:

أ) إنشاء فريق أمني:

- **تشكيل فريق أمني:** تشكيل فريق أمني مخصص لحماية الشخص وعائلته.
- **تحديد المهام:** تحديد المهام والمسؤوليات لكل فرد في الفريق.
- **تدريب الفريق:** تدريب الفريق على أساسيات الحماية.
- **التنسيق:** التنسيق بين أفراد الفريق.

ب) إنشاء خطط طوارئ:

- **خطط هروب:** إنشاء خطط هروب محددة مسبقاً.
- **خطط إخلاء :** إنشاء خطط إخلاء محددة مسبقاً.
- **خطوط اتصال:** إنشاء خطوط اتصال محددة مسبقاً.
- **ملاذات آمنة:** إنشاء ملاذات آمنة محددة مسبقاً.

ج) إنشاء شبكة اتصال:

- **شبكة اتصال آمنة:** إنشاء شبكة اتصال آمنة بين الشخص وعائلته.
- **قنوات اتصال:** إنشاء قنوات اتصال آمنة مع الجهات الأمنية.
- **قنوات اتصال:** إنشاء قنوات اتصال آمنة مع الأصدقاء الموثوقين.
- **قنوات اتصال:** إنشاء قنوات اتصال آمنة مع الحركة.

2- الإجراءات التدريبية:

أ) تدريب الشخص:

- **تدريب على الحماية:** تدريب الشخص على أساسيات الحماية.
- **تدريب على الهروب:** تدريب الشخص على أساسيات الهروب.
- **تدريب على المواجهة:** تدريب الشخص على أساسيات المواجهة.

- **تدريب على النجاة:** تدريب الشخص على أساسيات النجاة.

ب) تدريب العائلة:

- **تدريب على الحماية:** تدريب العائلة على أساسيات الحماية.
- **تدريب على الهروب:** تدريب العائلة على أساسيات الهروب.
- **تدريب على الاتصال:** تدريب العائلة على أساسيات الاتصال الآمن.
- **تدريب على النجاة:** تدريب العائلة على أساسيات النجاة.

ج) تدريب الفريق الأمني:

- **تدريب على الحماية** :تدريب الفريق الأمني على أساسيات الحماية
- **تدريب على الهروب** :تدريب الفريق الأمني على أساسيات الهروب
- **تدريب على المواجهة** :تدريب الفريق الأمني على أساسيات المواجهة
- **تدريب على النجاة** :تدريب الفريق الأمني على أساسيات النجاة

3- الإجراءات النفسية:

أ) الاستعداد النفسي:

- **الصبر:** الصبر والتحمل في الظروف الصعبة.
- **التوكل:** التوكل على الله في كل الأوقات.
- **التحدي:** التحدي في وجه الهجمات.
- **الاستعداد النفسي:** الاستعداد النفسي للمواجهة.

ب) الدعم النفسي:

- **الدعم النفسي:** تقديم الدعم النفسي للشخص.
- **الدعم النفسي:** تقديم الدعم النفسي للعائلة.
- **الدعم النفسي:** تقديم الدعم النفسي للفريق الأمني.
- **الدعم النفسي:** تقديم الدعم النفسي للأصدقاء الموثوقين.

ج) التأهيل النفسي:

- **التأهيل النفسي:** تأهيل الشخص نفسياً للمواجهة.
- **التأهيل النفسي:** تأهيل العائلة نفسياً للمواجهة.
- **التأهيل النفسي:** تأهيل الفريق الأمني نفسياً للمواجهة.
- **التأهيل النفسي:** تأهيل الأصدقاء الموثوقين نفسياً للمواجهة.

رابعا/ الإضافات المهمة لحماية الشخص وعائلته:

1- استخدام التكنولوجيا الذكية في الحماية:

أ) أنظمة التنبيه المبكر:

- **تطبيقات التنبيه:** استخدام تطبيقات التنبيه الفوري (مثل تطبيقات الطوارئ).
- **أنظمة المراقبة:** أنظمة المراقبة الذكية التي تراقب الحركات غير الطبيعية.
- **أجهزة التنبيه:** أجهزة التنبيه الصوتية والبصرية.
- **الشبكات الاجتماعية:** استخدام الشبكات الاجتماعية للتنبيه الفوري بطريقة ذكية متفق عليها.

ب) أنظمة التشفير المتقدمة:

- **تطبيقات التشفير:** استخدام تطبيقات التشفير الفوري (مثل: Signal – Telegram).
- **تشفير الملفات:** تشفير جميع الملفات والمعلومات الحساسة.
- **تشفير الاتصالات:** تشفير جميع الاتصالات (صوت، فيديو، نص).
- **تشفير الأجهزة:** تشفير جميع الأجهزة (هواتف، أجهزة كمبيوتر).

ج) أنظمة التخفي الذكي:

- **تطبيقات التخفي:** استخدام تطبيقات التخفي الذكية.
- **أنظمة تغيير المظهر:** أنظمة تغيير المظهر الذكية.
- **أنظمة تغيير الصوت:** أنظمة تغيير الصوت الذكية.
- **أنظمة تغيير الموقع:** أنظمة تغيير الموقع الذكية.

2- الاستعانة بالخبراء والمتخصصين:

أ) الاستعانة بخبراء الأمن:

- **استشارة الخبراء:** استشارة خبراء الأمن لوضع خطط الحماية.
- **استعانة بالخبراء:** استعانة بالخبراء لتنفيذ خطط الحماية.
- **متابعة الخبراء:** متابعة الخبراء لتحديث خطط الحماية.
- **التعاون مع الخبراء:** التعاون مع الخبراء لتحسين خطط الحماية.

ب) الاستعانة بخبراء التكنولوجيا:

- **استشارة الخبراء:** استشارة خبراء التكنولوجيا لوضع خطوط الحماية التقنية.
- **استعانة بالخبراء:** استعانة بالخبراء لتنفيذ خطوط الحماية التقنية.
- **متابعة الخبراء:** متابعة الخبراء لتحديث خطوط الحماية التقنية.
- **التعاون مع الخبراء:** التعاون مع الخبراء لتحسين خطوط الحماية التقنية.

ج) الاستعانة بخبراء النفس:

- **استشارة الخبراء:** استشارة خبراء النفس لوضع خطط الدعم النفسي.
- **استعانة بالخبراء:** استعانة بالخبراء لتنفيذ خطط الدعم النفسي.
- **متابعة الخبراء:** متابعة الخبراء لتحديث خطط الدعم النفسي.
- **التعاون مع الخبراء:** التعاون مع الخبراء لتحسين خطط الدعم النفسي.

3- الاستفادة من الخبرات السابقة:

أ) دراسة الحالات السابقة:

- **دراسة الحالات:** دراسة الحالات السابقة للاستهداف.
- **تحليل الحالات:** تحليل الحالات السابقة لاستخلاص الدروس.
- **تطبيق الدروس:** تطبيق الدروس المستفادة من الحالات السابقة.
- **تحسين الخطط:** تحسين خطط الحماية بناءً على الدروس المستفادة.

ب) الاستفادة من الخبرات الشخصية:

- **دراسة الخبرات:** دراسة الخبرات الشخصية للاستهداف.

- **تحليل الخبرات:** تحليل الخبرات الشخصية لاستخلاص الدروس.
- **تطبيق الدروس:** تطبيق الدروس المستفادة من الخبرات الشخصية.
- **تحسين الخطط:** تحسين خطط الحماية بناءً على الدروس المستفادة.

ج) الاستفادة من الخبرات الأمنية:

- **دراسة الخبرات:** دراسة الخبرات الأمنية للاستهداف.
- **تحليل الخبرات:** تحليل الخبرات الأمنية لاستخلاص الدروس.
- **تطبيق الدروس:** تطبيق الدروس المستفادة من الخبرات الأمنية.
- **تحسين الخطط:** تحسين خطط الحماية بناءً على الدروس المستفادة.

4- الجوانب النفسية والروحية:

أ) التوكل على الله:

- **الدعاء:** الدعاء المستمر والصادق.
- **الاستعانة بالله:** الاستعانة بالله في كل الأوقات.
- **التوكل على الله:** التوكل على الله في كل الأحوال.
- **الثقة بالله:** الثقة بالله في كل الظروف.

ب) الصبر والتحمل:

- **الصبر على البلاء:** الصبر على البلاء والشدائد.
- **التحمل في الظروف:** التحمل في الظروف الصعبة.
- **الصبر على الأذى:** الصبر على الأذى والظلم.
- **التحمل في الشدة:** التحمل في الشدة والرخاء.

ج) التضحية في سبيل الله:

- **التضحية بالنفس:** التضحية بالنفس في سبيل الله.
- **التضحية بالممتلكات:** التضحية بالممتلكات في سبيل الله.
- **التضحية بالراحة:** التضحية بالراحة في سبيل الله.
- **التضحية بالأمان:** التضحية بالأمان في سبيل الله.

5- الجوانب العملية الإضافية:

أ) التنقل الذكي:

- **التنقل في أوقات مختلفة:** التنقل في أوقات مختلفة عن المعتاد.
- **التنقل في طرق مختلفة:** التنقل في طرق مختلفة عن المعتاد.
- **التنقل في أماكن مختلفة:** التنقل في أماكن مختلفة عن المعتاد.
- **التنقل بشكل عشوائي:** التنقل بشكل عشوائي غير متوقع.

ب) الاختباء الذكي:

- **الاختباء في أماكن مزدحمة:** الاختباء في أماكن مزدحمة.
- **الاختباء في أماكن معروفة:** الاختباء في أماكن معروفة آمناً.
- **الاختباء في أماكن جديدة:** الاختباء في أماكن جديدة غير معروفة.

- **الاختباء بشكل مبتكر:** الاختباء بشكل مبتكر وغير تقليدي.

ج) التعامل مع الأزمات:

- **الهدوء في الأزمات:** الحفاظ على الهدوء في الأزمات.
- **التصرف بسرعة:** التصرف بسرعة في الأزمات.
- **اتخاذ القرار الصحيح:** اتخاذ القرار الصحيح في الأزمات.
- **التعامل بفعالية:** التعامل بفعالية في الأزمات.

الخلاصة:

- الإجراءات الفورية هي الأهم فوراً عند الشعور بالخطر.
- الإجراءات لمدة 24 ساعة هي الأهم بعد الإجراءات الفورية.
- الإجراءات طويلة الأمد هي الأهم لضمان الاستمرارية.
- الاستعداد هو مفتاح نجاح الحماية في كل الأوقات.
- التكنولوجيا هي الأداة المساعدة في الحماية، لكنها لا تغني عن الإعداد البشري.
- الخبراء هم المصدر الرئيس لوضع خطط الحماية، لكنها لا تغني عن الإعداد الذاتي.
- الخبرات هي المصدر الأساسي لاستخلاص الدروس، لكنها لا تغني عن الإعداد المستمر.
- التوكل على الله هو أساس الحماية، لكنه لا يغني عن الإعداد العملي.

القسم الثاني: القسم التطبيقي

(ما حدث في الضاحية الجنوبية من تفجيرات البيجرات والوكي توكي في سبتمبر 2024).

الاستهدافات الصهيونية في الضاحية الجنوبية وغيرها، نتناولها بالإجابة عن (4) أربعة أسئلة هي:

السؤال الأول: كيف يتم تحديد موقع هاتف مغلق داخل مبنى؟

السؤال الثاني: كيف يعمل الصاروخ داخل المبنى؟ وكيف تظهر فتحات متعددة؟

السؤال الثالث: كيف حصل الاختراق في عملية حارة حريك بالضاحية الجنوبية؟

السؤال الرابع: ما هي خطة الحماية العملية لمنع تكرار هذه الاغتيالات؟

وتاليا شرحها بشيء من التفصيل.

السؤال الأول: كيف يتم تحديد موقع هاتف مغلق داخل مبنى؟

جواب:

تعد هذه من أخطر التقنيات الحديثة، وبيانها بالآتي:

أولاً: الهاتف المغلق فعليًا لا ينطفئ بالكامل، هو يدخل في حالة اسمها:

Low-Power Mode / Deep Sleep

وفي هذه الحالة يبقى:

- الـ IMSI قابلًا للالتقاط.
- الـ IMEI يبثّ "نقطة حياة" كل 30–90 ثانية.
- البطارية تشغّل دوائر بسيطة جدًا.
- هذا يكفي لتحديد مكان الهاتف.

ثانيًا: تحديد الموقع عبر الطائرات الإسرائيلية فوق الضاحية، إسرائيل تنشر:

طائرات Hermes 900 – Heron – Eitan

وهذه الطائرات تحتوي على أجهزة:

IMSI catchers تحدد مكان الهاتف بدقة: من 1 إلى 3 أمتار، حتى لو كان مغلقًا، حتى لو كان من دون شريحة SIM.

وبعد تحديد إشارة الهاتف، تستطيع معرفة: الطابق – الغرفة – مكان الشخص داخل الشقة.

كيف يعرفون "الطابق"؟

من خلال قوة الإشارة وانعكاسها على الجدران (Signal Mapping).

ثالثًا: Wi-Fi mapping – حتى لو لم يتصل الهاتف بأي شبكة، يكفي:

اقترابه من راوتر – أو مروره قرب شبكة Wi-Fi – ليتم تحديد موقعه بدقة.

إسرائيل تمسح كل شبكات Wi-Fi في الضاحية باستمرار.

رابعًا: تحليل "ذبذبات الحركة" داخل المبنى؛ هناك تقنيات أميركية/ إسرائيلية اسمها:

Through-Wall Tracking تستخدم:

رادارات متنقلة – موجات ميكروويف – موجات mmWave

هذه تستطيع حساب: عدد الأشخاص – أماكنهم – نمط تنفسهم (!)
هذه التقنية استخدمت أواخر 2023 في غزة بشكل مكثف.

السؤال الثاني: كيف يعمل الصاروخ داخل المبنى؟ وكيف تظهر فتحات متعددة؟

الجواب:

الصواريخ المزودة بـ Side–Thrust أو شفرات اختراق لديها قدرات غير عادية:

1) تدخل من الجدار بدقة 10–30 سم وذلك بسبب: توجيه بصري – أجهزة تحكم من الطائرات – نظام GPS عالي الدقة.

2) بعد الدخول، يغير الصاروخ اتجاهه، يستخدم:

محركات جانبية صغيرة – دفع موجّه – زعانف تغيير زاوية المسار.

هذا يسمح له بالتحرك يمينًا أو يسارًا، أو صعودًا متراً أو مترين؛ وهذا ما يسبب ثقوبًا متعددة في الجدران.

3) يتجه نحو الحرارة البشرية: رأس التوجيه الحراري للسلاح يبحث عن:

مصدر حرارة – حركة الجسم – الكثافة البشرية في الزاوية المعينة.

ولذلك يصيب "الغرفة المقصودة" دون غيرها.

السؤال الثالث: كيف تحمي البيئة نفسها من هذه الاغتيالات؟

هذه أهم نقطة:

أولًا: الهواتف:

لا يكفي إطفاء الهاتف، يجب إزالته بالكامل، دون أي جهاز إلكتروني داخل غرفة الاجتماعات، حتى الساعة الذكية تشكل خطراً.

ثانيًا: تعطيل المباني من داخلها:

فصل الكهرباء في وقت الاجتماعات – عدم تشغيل Wi–Fi – عدم تشغيل تلفزيون ذكي – عدم تشغيل مكيفات أو أجهزة تبث حرارة غير بشرية.

ثالثًا: عزل النوافذ والواجهات بالكامل:

وضع ستائر حرارية Thick Curtains – إضافة ألواح خشبية داخلية – منع أي نافذة من أن تكشف حركة داخلية.

رابعًا: لا يجب أبدًا عقد اجتماع ثابت في المكان نفسه: العدو يحفظ النمط ويقتل كل من يحضر.

خامسًا: تفتيش المبنى كل أسبوعين بحثًا عن:

أجهزة GPS – كاميرات صغيرة – وحدات إرسال بحجم كفّ اليد.

السؤال الرابع: كيف حصل الاختراق في عملية حارة حريك بالضاحية الجنوبية؟

الجواب:

تحليل شامل ودقيق للمحاور الثلاثة، بالاعتماد على خبرة إسرائيل الطويلة في الاغتيالات داخل بيئات سكنية مكتظة مثل الضاحية وغزة ودمشق. المحاور الثلاثة هي:

المحور الأول: كيف حصل الاختراق في عملية حارة حريك؟

المحور الثاني: كيف عرفت إسرائيل بوجود 5 قادة معًا في لحظة واحدة؟

المحور الثالث: ما هي خطة الحماية العملية لمنع تكرار هذا النوع من الاغتيالات؟

وتفصيلات المحاور الثلاثة، كما تُفكّر بها غرف عمليات العدو بالآتي:

عملية بهذا الحجم – قتل 5 قادة + إصابة مدنيين + إصابة دقيقة داخل شقة – لا يمكن أن تنجح بدون اختراق مسبق.

في العمليات التي حصلت خلال السنوات الماضية، هناك (4) أربع طرق رئيسة للاختراق؛ وفي عملية حارة حريك، الاحتمال الأرجح هو تداخل ثلاثة منها معًا:

أولاً: اختراق الهاتف أو الأجهزة الإلكترونية داخل الشقة:

إسرائيل تعتمد على استغلال: الهواتف الشخصية – أجهزة Wi-Fi – كاميرات داخل المبنى – لابتوب مفتوح – تلفزيون ذكي – ساعة ذكية.

يكفي أن يكون هاتف واحد مضبوط على الوضع الساذج (غير محمي) ليقول للعدو:

من يدخل – من يخرج – عدد الأجهزة في الشقة – حرارة الحركة – موقع التحرك داخل كل غرفة– وقت انعقاد الاجتماع – مدة الاجتماع.

ثانيًا: معرفة الشقة تحديدًا وليس فقط المبنى: هذا يتم عبر:

- تتبع إشارة الهاتف (حتى لو كان مغلقًا) عبر طائرات IMSI.
- تحليل شبكة Wi-Fi الخاصة بالشقة.
- قراءة استهلاك الكهرباء في غرفة التجمّع.
- تصوير حراري من المسيّرات.

بهذه الطريقة يحصل على:

رقم الطابق – رقم الغرفة – مكان الجلوس داخل الغرفة.

ثالثًا: مراقبة حيّة من طائرة مسيّرة فوق الضاحية:

في عملية حارة حريك كان مؤكدًا وجود طائرة:

تراقب المدخل – ترصد حركة دخول القادة – وتلتقط صورًا حرارية للغرفة.

هذه المسيّرة ترسل:

عدد الأشخاص في الغرفة – من يجلس إلى جانب من – الجلسة قد بدأت أم لا

رابعًا: معلومة بشرية غير مباشرة:

ليس شرطًا وجود عميل مباشر؛ أحيانًا تكون المعلومة من:

عامل صيانة – صاحب محل في الشارع – جار يصوّر الحركة على واتساب – ساكن ينشر صورة لباب أو درج المعلومة البسيطة تكمل "صورة الإحداثيات" لدى العدو.

السؤال الخامس: كيف عرفت إسرائيل بوجود (5) خمسة قادة معًا في لحظة واحدة؟

الجواب:

هذه هي النقطة الأخطر في الاغتيال. فللعدو (4) أربع أدوات رئيسية تجعله يعرف "بالتمام والكمال" وجود اجتماع حساس:

أولا/ تجمّع إشارات الهواتف: حتى لو كانت الهواتف مغلقة، العدو يلتقط:

IMSI – IMEI – إشارة بعض الأجهزة التي تظل حيّة رغم الإغلاق.

إذا ظهر فجأة داخل شقة واحدة: 5 إشارات مختلفة المعروفة لدى العدو بأنها تعود لأشخاص محددين، فالنتيجة: إسرائيل تعرف خلال أقل من دقيقة أن اجتماعًا استثنائيًا حصل.

هذا وحده كافٍ لضربة فورية.

ثانيا/ تحليل حركة الأشخاص قبل الوصول إلى الشقة: إسرائيل تتابع (تتبع):

مسار كل قائد – اتجاه مشيته – نقاط التقاء غير متوقعة.

فإذا:

خرج قائد من نقطة A – وصل إلى منزل معروف بأنه آمن – ثم تبعه قائد آخر... ثم ثالث...

تعتبر إسرائيل هذا:

اجتماعًا عالي القيمة (High Value Meeting).

وهي تنتظر عادة اجتماعًا كهذا.

ثالثا/ كاميرات الطائرات المسيّرة فوق الضاحية: هذه الكاميرات:

تقرأ حرارة الأشخاص – تعرف حتى "طول" الشخص ونمط مشيته – تقيس عدد الأجساد داخل الشقة – تلتقط النوافذ والستائر.

عندما ترى:

لمبات ضوء تُضاء + حركة كثيفة + ستارة تحركت + خمسة أشخاص في دائرة واحدة

تعرف أن اجتماعًا مهمًا بدأ.

رابعا/ اختراق جهاز ذكي داخل الغرفة: هناك معلومات تشير إلى احتمال أن يكون:

تلفزيون ذكي – smart speaker – أو كمبيوتر

تعطي معلومات صوتية أو حرارية للعدو.

لا تحتاج إسرائيل لميكروفون. تحتاج فقط:

مقياس حرارة – أو تحليل اهتزاز الجدار – أو عدّ الذبذبات التي تنتج عن كلام عدة أشخاص

هذه كافية لتحديد عدد الأشخاص في الغرفة ومكان جلوسهم.

السؤال السادس: ما هي خطة الحماية العملية لمنع تكرار هذه الاغتيالات؟

جواب:

خطة عملية تعتمدها حركات مقاومة في عدة دول، وتتوافق مع الدروس التي تتعلمها البيئة الشعبية بعد كل اغتيال. الخطة مقسّمة إلى (3) ثلاث دوائر حماية:

الدائرة الأولى: حماية المعلومات قبل الوصول:

1) إلغاء الاجتماعات الثابتة: العدو ينتظر "نمطًا ثابتًا".

يجب أن تكون الاجتماعات: غير ثابتة – غير متوقعة – غير دورية.

2) عزل الهواتف بالكامل: ليس إغلاق الهاتف.

بل: تركه خارج المكان 30 مترًا على الأقل – أو وضعه داخل صندوق Faraday – منع الساعات الذكية، AirPods، الأجهزة الطبية.

3) تغيير طرق التنقل: لا يجب أن يسلك القادة:

نفس الطريق – نفس الدرج – نفس المصعد – نفس التوقيت

4) منع إدخال أي جهاز إلكتروني إلى غرفة الاجتماعات: حتى لو كان:

راوتر – لمبة Wi-Fi – شاشة – مكيّف – سبيكر

الدائرة الثانية: حماية المبنى:

1) فحص أسبوعي للغرف المشتركة: البحث عن:

كاميرا صغيرة – جهاز GPS – جهاز بثّ – microchip

هذه كلها تُترك في: درج – كوع سقف – علبة كهرباء – فوهة مكيف – زوايا الدرج

2) منع أي عمل صيانة غير معروف المصدر: العدو كثيرًا ما يزرع أجهزة خلال:

تصليح المصعد – تركيب ستالايت – تنظيف الواجهة – تمديدات الكهرباء.

3) عزل النوافذ بستائر حرارية مُحكَمة: لمنع التصوير الحراري.

4) تعمية Wi-Fi بالكامل وإطفاؤه قبل أي اجتماع.

الدائرة الثالثة: الحماية أثناء الاجتماع:

1) الاجتماع في غرفة بلا نوافذ: أكثر مكان آمن:

غرفة داخلية – بلا شباك – بلا أجهزة كهربائية – بلا سقف معدني.

2) تغيير مكان الاجتماع كل مرة، حتى ضمن المبنى نفسه.

3) إطفاء الكهرباء في الغرفة لمنع:

إشارات Wi-Fi غير المقصودة – إشعاع الأجهزة – كاميرات ذكية.

4) مراقبة الطائرات المسيّرة قبل البدء: إذا كانت هناك طائرة تحلق فوق المنطقة بشكل ثابت:

لا اجتماع.

الخلاصة:

الاغتيالات التي تمت في الضاحية لا تعتمد على "سلاح خارق فقط"، بل على منظومة كاملة من:

1. تجسس إلكتروني مكثف.
2. اختراق الأجهزة داخل المنازل.
3. تعقّب الهواتف حتى لو كانت مغلقة.
4. مسّاح Wi-Fi ورادارات تركّز على كل بناء.
5. سلاح دقيق جدًا يقود نفسه داخل المبنى.
6. مناورة داخل الغرف قبل الانفجار.
7. غرفة عمليات إسرائيلية تشاهد كل شيء لحظة التنفيذ.
8. هذه ليست عملية عشوائية ... بل هي "عملية جراحية"، عادة تتم بعد أسابيع من المراقبة الدقيقة.

9. اغتيال حارة حريك لم يكن بسبب سلاح خارق فقط. بل بسبب:

اختراق معلوماتي – تعقب إلكتروني – مراقبة حرارية – معرفة مسبقة بالشقة والغرفة – اجتماع مفاجئ لأشخاص مهمين.

10. وفي المقابل: البيئة قادرة على تقليل هذه الاغتيالات بنسبة 70–80% لو طبّقت الخطوات المذكورة أعلاه.

كيف تتجنب الاستهداف؟

....

ولأن الحماية من الاستهداف هو علم بحد ذاته مبني على معرفة الكثير من الأدوات واني يقوم عليها الاستهداف، ولأن معرفة تجنب الاستهداف يصبح بمنزلة الفرض على بعض الأشخاص (إن لم يكن كذلك على جميع القاطنين في مناطق النزاع والتعرض الخطر): بذلك يصبح على بعض الأشخاص (والأفضل الجميع) البحث والكشف عن كيفية تجنب الاستهداف، وجعلها ثقافة له ولأفراد عائلته وللمقربين والمتعاملين معه.

تم تقسيم هذه الورقة إلى قسمين يتم الإجابة من خلالهما على أسئلة تتضمن موضوع الاستهداف، وبيان ذلك بالآتي:

القسم الأول: القسم النظري:

السؤال الأول: شاهدنا الأيام الماضية كيف يتم استهداف شخصيات كثيرة بصواريخ وبغيرها، فكيف يتم تحديد الشخص المستهدف؟ وكيف يعرف انه مستهدف؟ وكيف يحمي نفسه من الاستهداف؟

السؤال الثاني: إذا شعر الشخص انه مستهدف، ما هي الاجراءات التي يتخذها لحماية نفسه أولا، ثم عائلته الملازمين له؟

القسم الثاني: القسم التطبيقي

(ما حدث في الضاحية الجنوبية من تفجيرات البيجرات والوكي توكي في سبتمبر 2024).

1. كيف يتم تحديد موقع هاتف مغلق داخل مبنى؟
2. كيف يعمل الصاروخ داخل المبنى؟ وكيف تظهر فتحات متعددة؟
3. كيف حصل الاختراق في عملية حارة حريك بالضاحية الجنوبية؟
4. ما هي خطة الحماية العملية لمنع تكرار هذه الاغتيالات؟



